CAPINTECH

Remote Access Trojans (RATs): Why We Cover Our Webcams

By Lisa Traina, Partner

When speaking on encryption and surveillance at Kenyon College in April 2016, James Comey, then the director of the FBI, divulged that he'd placed a piece of tape over the camera on his personal computer.

And after Facebook chairman and CEO Mark Zuckerberg posted a photo that showed his work computer in June 2016, thousands of people noticed that he had tape over his MacBook camera and microphone.

So why would the director of the FBI and the founder of Facebook resort to placing tape over the cameras and microphones at their personal workstations?

The answer is RATs — remote access Trojans.

What Are RATs?

Almost everyone in business today is familiar with remote desktop applications such as LogMeIn, TeamViewer, GoToMeeting, WebEx, and Bomgar. These enterprise tools provide remote access to a system and are useful and efficient ways to cut operating costs, ensure fast response time with help desks, or just get that much-needed document from your workplace when you are out of the office.

RATs are a malicious variant of these remote access tools — custom-created software the user can execute to control any system without the victim's knowledge.

One of the first RATs was made public in 1999, and in the years since RATs have become more sophisticated through obfuscation. Today, most of the popular RATs are capable of performing keylogging, screen and camera capture, file access, code execution, registry management, password sniffing, and more. Through persistence, an attacker can run malware, exfiltrate data from the victim, and sell the data or use it to extort the victims at a later date.

RATs can be installed on a system through phishing links, email attachments, ransomware, infected USB drives, and more. They are custom-built to evade antivirus programs, intrusion detection, and prevention products (IDS/IPS) and are sold relatively cheaply on clearnet hacking forums and the dark web.

How Big is the Threat?

In the hierarchy of cybercrime, RATs are near the top. There are dozens of different techniques that cybercriminals use to keep their RATs from being detected.

RATS can be "binded," or merged, into a legitimate program using very basic tools. The most popular are Adobe Flash, Google Chrome installers, and any web-based or local installer trusted by the workstation or domain. This is what makes a RAT unknown and undetectable to antivirus vendors.

> In the hierarchy of cybercrime, RATs are near the top.

But the role of the RAT, like any creative virus, is to be persistent even after detection. Ten minutes of a target being "ratted" is more than enough time to upload multiple backdoors into a network that can stay persistent long after the RAT is discovered and eradicated, allowing future attacks. Ten minutes is also enough time to gain sufficient data to use in ransoming, extorting, or threatening an individual or business. The details of extortion techniques are changing on a monthly basis.

6 Steps to Help Protect Your Organization

There will never be a product that fully protects any person or organization from RATs, viruses, malware, exploits, zero-day vulnerabilities, or other cyber threats. At this stage, the best prevention against RATs is for your

organization to follow these best practices recommended by security researchers, engineers, and coders:

1. Do not save unencrypted private information on a home or organization workstation. Encrypt your files with fully audited open source VeraCrypt and AXCrypt (if you access remote). These provide multiple features and 99.99% chance of no government backdoors with access to the encryption key.
2. Train everyone with access to your network on the importance of avoiding unsafe websites, particularly sites that are ad-driven and full of pop-ups, as these may contain a drive-by RAT waiting to be deployed.
3. Ensure your organization performs daily backups with minimum 256-bit AES encryption and redundant data eliminated (de-duplicated). These backups should be replicated off-site.
4. Watch your firewall, IDS/IPS logs for unusually large amounts of data being offloaded out. That is one of the biggest clues that your network has been penetrated. Basic network security should have egress filtering already in place with quality of service (QoS) controls to alert of such patterns.
5. Use multi-factor authentication and print out the backup codes when you are offsite from your network. This is to prevent account takeovers if you have been compromised.
6. Use your AV, IDS/IPS appliances and software and review the reports, especially those sent on the weekend. Most cybercrimes occur starting after hours on Friday afternoon, so customize your alerts to be a little more detailed during those times.

Also consider covering webcams and microphones when they're not in use. If a RAT is used to activate them, the cybercriminals won't be able to glean useful information.

Cybercrime has been unleashing significant destruction. The sinister nature of daily exploits, leaks, and hacks is numbing even the most hardened security researchers, and it seems the end is not in sight. While emerging technologies might be helpful in the fight against RATs in the future, for now your best protection is to follow the best practices above and layer your cybersecurity controls so that if one fails, others can help protect your organization.

CapinTech can help you assess your organization's cybersecurity risk and provide recommendations to help you reduce it. Please contact us at cybersecurity@capincrouse.com to discuss your specific needs.

This article was orginally published in The NonProfit Times.

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.